Amendments to the claims:

1   1. (previously cancelled)

2   2. (previously cancelled)

     3. (previously cancelled)

     4. (previously cancelled)

     5. (previously cancelled)

     6. (previously cancelled)

     7. (previously cancelled)

     8. (previously cancelled)

     9. (previously cancelled)

1   10. (currently amended) Data protection method for operating a
2   microprocessor of a chip card to protect data elements contained in
3   a memory of a chip card from discovery by analysis of electrical
4   power consumption by the microprocessor, said method using a
5   cryptographic algorithm for executing operations for processing
6   said data elements so as to generate encrypted information, said
7   method comprising:

8   operating the microprocessor to randomly modifying the
9   order of execution of operations involving
10   manipulations of data elements contained in the
11   memory from one cycle to another, a cycle being a
12   complete execution cycle of the algorithm or an
13   intermediate cycle of a group of operations, said
14   operations being operations whose order of execution
15   relative to the others does not affect the result,
16   thereby protecting said data elements contained in
17   said memory and processed by a microprocessor in a

M481-6 Amendment v12.doc

18   chip card from discovery by analysis of the

19   microprocessor's electric power consumption.

1   11. (currently amended) The protection method according to claim 10,

2   wherein the modified order of execution of operations include

3   permutation of bits of a message block ~~before~~ which is performed

4   after the permutation of bits of a key, and vice versa.

1   12. (currently amended) The protection method according to claim 10,

2   wherein the modified order of execution of operations include a

3   random determination of the processing of quartets~~modifying the~~

4   ~~order of processing quartets making up a data element~~.

1   13. (cancelled)

1   14. (Currently Amended) Data protection method for operating a

2   microprocessor of a chip card to protect data elements contained in

3   a memory of the chip card from discovery by analysis of the electric

4   power consumption of the microprocessor, said method using a

5   symmetric cryptographic algorithm of the DES-type with a

6   permutation step for executing operations for processing data

7   elements so as to generate encrypted information, said method

8   comprising:

9   operating the microprocessor to ~~using a symmetric~~

10   ~~cryptographic algorithm of the DES-type with a~~

11   ~~permutation step, said permutation step including a~~

12   ~~random~~ randomly ~~determination~~ of determine a

13   processing order of the bits for the execution of the

14   permutation step, thereby protecting said data

15   elements ~~processed by a microprocessor in a chip card~~

16   from discovery by analysis of the microprocessor's

17   electric power consumption.

Page 3 of 19

M481-6 Amendment v12.doc

1   15. (previously presented) The data protection method of Claim 14
2   wherein the cryptographic algorithm for executing operations for
3   processing data elements includes a group of operations executed
4   repeatedly.

1   16. (new) The data protection method of Claim 10 wherein said data
2   elements are keys.

1   17. (new) The data protection method of Claim 10 wherein said data
2   elements are keys.

M481-6 Amendment v12.doc